UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/552,955	10/14/2005	Fredrik Lindholm	P18053-US1	2497

27045 7590 11/26/2010

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
NGUYEN, TRONG H	
ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
11/26/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

kara.coffman@ericsson.com
jennifer.hardin@ericsson.com
melissa.rhea@ericsson.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/552,955
Filing Date: October 14, 2005
Appellant(s): LINDHOLM ET AL.

Roger S. Burleigh
Reg. No. 40,542
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on 10/26/2010 appealing from the Office action mailed on 05/26/2010.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The following are the related appeals, interferences, and judicial proceedings known to the examiner which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal:

A prior appeal brief was filed for this application on 03/04/2010 appealing from the Final Office action mailed on 08/03/2009 and Advisory action mailed on 11/03/2009.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application: claims 1-11, 13-32 and 34-45.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

No separate heading/section for summary of claimed subject matter accompanied by specific references to the specification and reference characters in drawings is found in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The copy of the appealed claims contained in the claims appendix shows some claims being "Currently Amended" while there are no markings or amendments.

(8) Evidence Relied Upon

The following is a listing of the evidence (e.g., patents, publications, Official Notice, and admitted prior art) relied upon in the rejection of claims under appeal:

US 6,792,533	Jablon	09-2004
US 6,721,886	Uskela	04-2004
US 5,778,065	Hauser et al.	07-1998

US 6,397,329	Aiello et al.	05-2002
US 6,215,877	Matsumoto	04-2001
US 6,885,388	Gunter et al.	04-2005
US 7,363,494	Brainard et al.	04-2008
US 6,668,167	McDowell et al.	12-2003
US 7,076,656	MacKenzie	07-2006

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 10-11, 13, 39 and 42-45 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 10 recites “the token secret” on last line however it is unclear whether “the token secret” refers to “a token secret” recited on line 10 of claim 1 or “a token secret” recited on line 3 of claim 10. Similar issue also exists in claims 11 and 13.

Claim 39 recites “wherein policies defining critical operations for which authentication is needed” which is unclear. For examining purposes, it will be interpreted similarly to claim 21.

Claims 42-45 recite “the device" on line 1 however it is unclear whether "the device" refers to "first device" or some other device in "a group of at least two devices" in claim 41.

Claim 45 recites “the token secret” on last line however it is unclear whether “the token secret” refers to “a token secret” recited on line 12 of claim 41 or “a token secret” recited on line 3 of claim 45.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 1 is rejected under 35 U.S.C. 101 based on Supreme Court precedent and recent Federal Circuit decisions, a 35 U.S.C § 101 process must (1) be tied to a particular machine or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In re Bilski et al, 88 USPQ 2d 1385 CAFC (2008); Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584,588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S. 780,787-88 (1876).

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory process, the claim should positively recite the particular machine to which it is tied, for example by identifying the apparatus that accomplishes the method steps, or positively

recite the subject matter that is being transformed, for example by identifying the material that is being changed to a different state.

Here, applicants' method steps are not tied to a particular machine and do not perform a transformation. Thus, the claim is non-statutory.

The mere recitation of the machine in the preamble with an absence of a machine in the body of the claim fails to make the claim statutory under 35 USC 101. *Note the Board of Patent Appeals Informative Opinion Ex parte Langemyer et al.*

Claims 2-11 and 13-24 are rejected under 35 U.S.C. 101 as non-statutory for at least the reason stated above. Claims 2-11 and 13-24 depend on claim 1; however, they do not add any feature or subject matter that would solve any of the non-statutory deficiencies of claim 1.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 1, 10-11, 13, 15-21, 23, 25, 32, 34-41 and 45** are rejected under 35 U.S.C. 102(e) as being anticipated by Jablon US 6,792,533 B2 (hereinafter "Jablon").

Regarding claim 1, Jablon discloses **a method for password-based authentication in a communication system including a group of at least two units** [Fig. 5, col. 18, lines 55-59: authenticating Alice to Bob, where Bob is the host computer and Alice is the user's computer] **associated with a common password,** [Fig. 5: 501 C = shared password] **comprising the steps of**;

assigning individual authentication tokens [col. 19, line 65 - col. 20, line 2: each of Alice and Bob is assigned a one way hidden password $S = H_C(g)$] **to the respective units in the group based on the password such that each authentication token is irreversibly determined by the password**; [col. 19, line 65 – col. 20, line 2: the one way hidden password $S = H_C(g)$ is a one way function of the shared password C]

determining, at a first unit, a check token [Fig. 5, 505: W = proof (K_1, K_2)] **for a second unit based on the password inputted by a user of said first unit and the authentication token of the first unit**, **wherein the step of determining the check token comprises the steps of**;

determining, at the first unit, a token secret [Fig. 1 and col. 20, lines 3-5: the shared authenticated key K_1 is generated by Alice in the SPEKE exchange using the one way hidden password S which is a one way function of shared password C] **using the authentication token of the first unit and the password**; and,

creating, at the first unit, the check token [Figs. 1 and 5, 505, col. 20, lines 3-20: Alice computes W = proof (K_1, K_2) where the shared authenticated

key K_1 is generated in the SPEKE exchange using the one way hidden password S which is a one way function of shared password C] **for the second unit based on the token secret and the password**;

sending the check token to the second unit; [Fig. 5: 509 Alice sending W to Bob] and,

comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit, wherein said user of said first unit is authenticated if said check token is the same as said authentication token of said second unit. [Fig. 5, 515-517: after receiving W from Alice 509, Bob verifies that W proves that she knows both K_1 and K_2 515. If the verification succeeds, Bob has proven that Alice knows C and the protocol succeeds 517]

Regarding claim 10, Jablon further discloses **the method of claim 1, wherein the assigning step further comprises the steps of**;

determining, at an assigning unit in the group, a token secret common for the group and non-correlated with the password; [col. 19, lines 48-49: some fixed value g known to Bob and Alice] and,

creating, at the assigning unit, the authentication token for another unit in the group based on the token secret and the password [col. 19, line 65-67: Alice computes the one way hidden password $S = H_C(g)$]

Regarding claim 11, Jablon further discloses **the method of claim 10 wherein the step of determining the token secret involves generating the token secret, as part of an initial set-up procedure** [col. 19, line 64: at time of password setup]

Regarding claim 13, Jablon further discloses **the method of claim 10, wherein the creating step involves using a bijective locking function, the input parameters of which include the token secret and a one-way function of the password** [col. 7, lines 5-12 and col. 19, line 65-67: Alice computes the one way hidden password $S = H_C(g)$]

Regarding claim 15, Jablon further discloses **the method of claim 13, wherein the locking function is implemented through password-based secret sharing** [col. 7, lines 5-12 and col. 19, line 65-67: Alice computes the one way hidden password $S = H_C(g)$]

Regarding claim 16, Jablon further discloses **the method of claim 1, wherein implementing policies in at least one of the units in the group for limiting the number and/or frequency of authentication attempts** [col. 12, lines 8-17: logging failed attempts, counting the number of failed attempts over the lifetime of the password, disabling the password if a specific limit is exceeded, and temporarily disabling the account during a suspected attack count total failed attempts to detect attacks against anonymous accounts]

Regarding claim 17, Jablon further discloses t**he method of claim 1, further comprising the step of generating an alarm signal if the number of authentication attempts exceeds a predetermined value** [col. 12, lines 8-17: logging failed attempts, counting the number of failed attempts over the lifetime of the password, disabling the password if a specific limit is exceeded, and temporarily disabling the account during a suspected attack count total failed attempts to detect attacks against anonymous accounts]

Regarding claim 18, Jablon further discloses **the method of claim 1, further comprising the step of sending an authentication response message from the second unit indicating the result of the comparing step** [Fig. 5, Abort 516 or OK 517]

Regarding claim 19, Jablon further discloses **the method of claim 1, further comprising the step of authentication of the second unit towards the first unit, whereby the first and second units are mutually authenticated towards each other** [col. 22, lines 37-40, col. 23, lines 19 and 23: Bob is verified and Alice is verified]

Regarding claim 20, Jablon further discloses **the method of claim 19, further comprising the steps of:**

generating a respective random value at the first and second unit; [col. 23, lines 8 and 10: Bob generates a random integer R_B, Alice generates random integer R_A]

determining temporary test secrets at the first and second unit based on the random values; [col. 23, lines 8 and 12: Bob generates $Q_B = h(S)^{(2 R_B)} \bmod p$ and Alice generates $Q_A = h(S)^{(2 R_A)} \bmod p$] and,

exchanging the temporary test secrets between the first and second unit for mutual authentication purposes [col. 23, lines 8 and 13: Bob sends Q_B to Alice and Alice sends Q_A to Bob]

Regarding claim 21, Jablon further discloses **the method of claim 1, wherein critical operations for which authentication is needed are listed in policies in at least one of the units** [col. 24, lines 1-14: Since passwords are ubiquitous, this invention has broad applications. It is useful for enhanced security in situations where passwords or PINs are traditionally used, such as remote personal-computer banking, authenticating access for portable telephones, and in general, remote secure financial and other transactions. It is also suitable for general computer network login procedures, where the security of the underlying network may not be entirely trusted]

Regarding claim 23, Jablon further discloses **the method of claim 1, wherein the group of units constitutes a Personal Area Network (PAN)** [Fig. 1 or 5]

Regarding claim 25, this claim contains limitations that are substantially similar to those recited in claim 1 above and accordingly is rejected for similar reasons.

Regarding claim 32, this claim contains limitations that are substantially similar to those recited in claim 10 above and accordingly is rejected for similar reasons.

Regarding claim 34, this claim contains limitations that are substantially similar to those recited in claim 13 above and accordingly is rejected for similar reasons.

Regarding claim 35, this claim contains limitations that are substantially similar to those recited in claim 16 above and accordingly is rejected for similar reasons.

Regarding claim 36, this claim contains limitations that are substantially similar to those recited in claim 17 above and accordingly is rejected for similar reasons.

Regarding claim 37, this claim contains limitations that are substantially similar to those recited in claim 18 above and accordingly is rejected for similar reasons.

Regarding claim 38, this claim contains limitations that are substantially similar to those recited in claim 19 above and accordingly is rejected for similar reasons.

Regarding claim 39, this claim contains limitations that are substantially similar to those recited in claim 21 above and accordingly is rejected for similar reasons.

Regarding claim 40, this claim contains limitations that are substantially similar to those recited in claim 23 above and accordingly is rejected for similar reasons.

Regarding claim 41, this claim contains limitations that are substantially similar to those recited in claim 1 above and accordingly is rejected for similar reasons.

Regarding claim 45, this claim contains limitations that are substantially similar to those recited in claim 10 above and accordingly is rejected for similar reasons.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 2, 26 and 42** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of Uskela US 6,721,886 (hereinafter "Uskela").

Regarding claim 2, Jablon discloses **the method of claim 1** but does not specifically disclose **further comprising the step of: deleting the password and all significant parameters generated except the authentication tokens after usage thereof**.

However, Uskela discloses a method for preventing unauthorized use of services wherein authentication, verification, and user data generated during authentication are deleted from memory after authentication (Col. 5, lines 40-43).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the time of the invention to modify the invention of Jablon by deleting sensitive data such as user data (password), authentication and verification data (intermediate parameters) generated during authentication after usage except provided authentication tokens as described by Uskela since it would provide a safety measure against the security risk (Uskela, Col. 5, lines 39-40).

Regarding claim 26, this claim contains limitations that are substantially similar to those recited in claim 2 above and accordingly is rejected for similar reasons.

Regarding claim 42, this claim contains limitations that are substantially similar to those recited in claim 2 above and accordingly is rejected for similar reasons.

7. **Claims 3, 5, 27, 29 and 43** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of Hauser et al. US 5,778,065 (hereinafter "Hauser").

Regarding claim 3, Jablon discloses **the method of claim 1** but does not specifically disclose **further comprising the step of: accepting, at the second unit in response to a successful authentication, update information securely transferred from the first unit, at least a portion of the update information being created at the first unit**.

However, Hauser discloses an authentication server in response to a successful authentication, accepting update information (new key or password) securely transferred (encrypted under present key) from a user and the update information is created by the user (Col. 2, lines 31-32, 34-36, and 44).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jablon by having the second unit accepting update information securely transferred from the first unit in response to a successful authentication as described by Hauser for security reasons since passwords or keys are necessary to communicate safely between users or between users and servers (Hauser, Col.1, lines 13 and 22-24).

Regarding claim 5, Jablon-Hauser combination further discloses **the method of claim 3**, **wherein the update information relates to a password change** [Hauser, Col. 7, lines 10-11: discloses a user requesting a password change or update with an authentication server].

Regarding claim 27, this claim contains limitations that are substantially similar to those recited in claim 3 above and accordingly is rejected for similar reasons.

Regarding claim 29, this claim contains limitations that are substantially similar to those recited in claim 5 above and accordingly is rejected for similar reasons.

Regarding claim 43, this claim contains limitations that are substantially similar to those recited in claim 3 above and accordingly is rejected for similar reasons.

8. **Claims 4 and 28** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of Hauser and further in view of Aiello et al. US 6,397,329 (hereinafter "Aiello").

Regarding claim 4, Jablon-Hauser combination discloses **the method of claim 3** but does not specifically disclose **wherein the update information is associated with revocation of a non-trusted group member**.

However, Aiello disclose a certificate authority (CA) periodically generates and signs a complete certificate revocation list (CRL) or a modification of a previous list or revoked certificates (Col. 4, lines 13-16).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jablon-Hauser by having the update information associating with revocation of a non-trusted group members as described

by Aiello since it would provide for the purpose of verifying the authenticity of a presented identity (Aiello, Col. 6, lines 23-24).

Regarding claim 28, this claim contains limitations that are substantially similar to those recited in claim 4 above and accordingly is rejected for similar reasons.

9. **Claims 7-8, 31 and 44** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of Hauser and further in view of Matsumoto US 6,215,877 (hereinafter "Matsumoto").

Regarding claim 7, Jablon-Hauser combination discloses **the method of claim 3** but does not specifically disclose **further comprising the step of delegating update rights to a third intermediate unit, and sending at least a portion of the update information for the second unit to the intermediate unit**.

However, Matsumoto disclose a key management server generates a new channel secret key for a chat client, delegates update rights (right to transmit the new key to the chat client) to a chat server and transmits this newly generated channel secret key to the chat server to be sent to a chat client (Fig. 6, Col. 1, lines 61-64 and Col. 10, lines 45-49).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jablon-Hauser by delegating update

rights to a third intermediate unit as described by Matsumoto since it would provide for the purpose of preventing eavesdropping (Matsumoto, Col. 1, lines 42-44).

Regarding claim 8, Jablon-Hauser-Matsumoto combination further discloses **the method of claim 7, wherein the update information is accompanied by a time stamp for determining whether the update information is still valid when the intermediate unit encounters the second unit** as [Matsumoto, Col. 10, lines 45-49: discloses the deadline of the key is written in the channel secret key for determining the validity of the channel secret key. In addition, Hauser, Col. 2, lines 33 and 43-44: also discloses including freshness information in update information to determine its validity].

Regarding claim 31, this claim contains limitations that are substantially similar to those recited in claim 7 above and accordingly is rejected for similar reasons.

Regarding claim 44, this claim contains limitations that are substantially similar to those recited in claim 7 above and accordingly is rejected for similar reasons.

10. **Claim 9** is rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of Hauser, further in view of Matsumoto, and further in view of Gunter et al. US 6,885,388 (hereinafter "Gunter").

Regarding claim 9, Jablon-Hauser-Matsumoto combination discloses **the method of claim 7** but does not specifically disclose **wherein the delegation of update rights comprises delegation of rights to further delegate update rights**.

However, Gunter discloses delegation of permission comprises the authority to delegate one or more further permissions to subsequent delegates (Col. 2, lines 40-41).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jablon-Hauser-Matsumoto by having delegation of update rights comprises delegation of rights to further delegate as described by Gunter since it would provide for the purpose of secure and convenient distribution of sensitive content and services (Gunter, Col. 2, lines 23-24).

11. **Claim 14** is rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of Brainard et al. US 7,363,494 (hereinafter "Brainard").

Regarding claim 14, Jablon discloses **the method of claim 13** but does not specifically disclose **wherein the locking function is a symmetric encryption function**.

However, Brainard discloses that an authentication code may be generated by a block cipher which encrypts a hash value of a shared password and/or other additional values using a stored secret (K) (Brainard, Col. 10, lines 58-61, Col. 14, lines 65-67, and Col. 15, lines 1-2)].

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jablon by having the locking function being a symmetric encryption function as described by Brainard since it is well known in the art.

12. **Claim 22** is rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of Hauser and further in view of McDowell et al. US 6,668,167 (hereinafter "McDowell").

Regarding claim 22, Jablon-Hauser combination discloses **the method of claim 3** but does not specifically disclose **wherein a unit that is switched-on after being inactive for a predetermined period of time automatically requests appropriate update information from at least two other units**.

However, McDowell discloses a MS that is turned on after being inactive for a predetermined period of time automatically requests update information (new TMSI) from the MSC and VLR (Fig. 14, Col. 10, lines 54-55).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jablon-Hauser by having a unit after switched-on automatically requests update information as described by McDowell

since it would provide for the purpose of receiving important update information (McDowell, Col. 10, lines 54-55).

13. **Claim 24** is rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of MacKenzie US 7,076,656 (hereinafter "MacKenzie").

Regarding claim 24, Jablon discloses **the method of claim 1** but does not specifically disclose **wherein the authentication tokens are tamper-resistantly stored in the respective units**.

However, MacKenzie discloses persistent stored data being tamper-proof (Col. 2, lines 22-26).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jablon by tamper-proofing stored authentication codes (persistent stored data) in respective units as described by MacKenzie since it would provide extra security against attack by adversaries (MacKenzie, Col. 2, lines 27-29).

(10) Response to Argument

1) CLAIMS 1-11 and 13-24 ARE DIRECTED TO STATUTORY SUBJECT MATTER

On page 4 of the brief, Appellant argues that Claim 1 is directed to a "method for password-based authentication in a communication system including a group of at least

two units associated with a common password." (emphasis added) The steps in the method include functions explicitly recited to be performed in either a first or a second unit, as well as a transmission from the first unit to the second unit. Accordingly, claim 1 not only recites a "machine" in the preamble, but the steps are tied to particular machines within the body of the claim; claims 2-11 and 13-24, which are dependent from claim 1, include further elements tied to those particular machines. Therefore, claims 1-11 and 13-24 are directed to statutory subject matter.

In response, the examiner respectfully disagrees. Claims 1-11 and 13-24 fail the machine or transformation test as the steps recited in these claims could be performed in one's mind or manually without any apparatus. It should be noted that these claims reciting steps being performed "at" the first or second unit which could be reasonably interpreted as being performed “near” or “on” the first or second unit. Thus, claims 1-11 and 13-24 are non-statutory.

2) CLAIMS 1, 10, 11, 13, 15-21, 23, 25, 32, 34-41 AND 45 ARE NOT ANTICIPATED BY U.S. PATENT NO. 6,792,533 ("JABLON")

On pages 6-7 of the brief, Appellant argues that Claim 1 recites the first limitation of assigning **individual authentication tokens to the respective units in the group** *based on the password such that each authentication token is irreversibly determined by the password*; i.e., each unit in the group gets an individualized (i.e., unique) authentication token that is irreversibly determined by a common (i.e., shared) password. For that limitation, the Examiner points to column 19, line 65, to column 20,

line 2, and asserts that a "one way hidden password S=Hc(g) is a one way function of shared password C," which is illustrated in Figure 5 as element 533. It can be noted, however, that element 533 is only associated with the "Bob" unit (i.e., computer) and not the "Alice" unit. In other words, even if the "hidden password" taught by Jablon is equated to an "authentication token" as presented in claim 1, there is not an individualized "hidden password" associated with both units. Therefore, Jablon fails to teach assigning **individual authentication tokens to the respective units in the group** based on the password such that each authentication token is irreversibly determined by the password.

In response, the examiner respectfully disagrees. In response to Appellant's argument that the references fail to show certain features of Appellant's invention, it is noted that the features upon which Appellant relies (i.e., individualized means unique) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In addition, since the instant specification does not specifically define "individual", under the broadest reasonable interpretation consistent with the instant specification, the examiner interprets "individual" to be each unit individually possesses a copy of an item. Furthermore, Jablon discloses that Alice (first unit) stores a copy of one way hidden password S and Bob (second unit) also stores a copy of one way hidden password S (col. 19, line 54 - col. 20, line 5). Jablon further discloses that one way hidden password S = Hidden (C) = $H_C(g)$ is a one way function of a shared password C

(col. 19, lines 46-49). Thus, Jablon does disclose assigning **individual authentication tokens to the respective units in the group** based on the password such that each authentication token is irreversibly determined by the password.

On page 7 of the brief, Appellant argues that the Examiner asserts that Jablon teaches the second claim element, "**determining, at a first unit, a check token for a second unit based on the password inputted by a user of said first unit and the authentication token of the first unit,**" referring to element 505 of Figure 5 (W = proof (K1, K2). As can be seen in Figure 5, and described at column 19, line 52, et seq., W is a function of a "Shared password" 501 and a "Key shared with Bob" 531; W is also a function of a "challenge" 512 received from Bob (U = Hx(g)). Thus, if the "Shared password" 501 is equated to the "password inputted by a user of a first unit," as recited in claim 1, then the "Key shared with Bob" 531 must be equated to the claimed "authentication token of the first unit." As described supra, however, the authentication tokens utilized in Applicant's invention are "individualized" (i.e., unique) to each unit and, therefore, are not shared. Therefore, Jablon also fails to teach "**determining**, at a ***first*** unit, **a check token *for a second unit* based on the password inputted by a user of said first unit and the authentication token of the *first* unit**."

In response, the examiner respectfully disagrees. In response to Appellant's argument that the references fail to show certain features of Appellant's invention, it is noted that the features upon which Appellant relies (i.e., the authentication tokens utilized in Applicant's invention are "individualized" (i.e., unique) to each unit and,

therefore, are not shared) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Moreover, Jablon discloses Alice generating W = proof (K_1, K_2) (check token) for Bob (Fig. 5: 505 and col. 21, lines 5-9) where K_1 (token secret) is generated by Alice in the SPEKE exchange based on Alice's stored copy of one way hidden password S = hidden(C) = $H_C(g)$ (authentication token of Alice) (col. 19, lines 54-59, col. 19, line 63 - col. 20, line 5, col. 7, lines 28-52 and Fig. 1) which is a one way function of shared password C (col. 19, lines 46-49). Note that when employing HVER method (Fig. 5), S (101) shown in Fig. 1 (SPEKE exchange) is Alice's stored copy of one way hidden password S and S (121) is Bob's stored copy of one way hidden password S (col. 19, lines 54-59 and col. 19, line 63 - col. 20, line 5). Thus, Jabon does disclose "**determining**, at a ***first*** unit, **a check token *for a second unit* based on the password inputted by a user of said first unit and the authentication token of the *first* unit**."

On pages 7-8 of the brief, Appellant argues that the Examiner asserts that Jablon teaches "**comparing**, at the second unit, **the check token** [**created by the first unit] *with the authentication token of the second unit*** for authentication of the first unit towards the second unit, ***wherein said user of said first unit is authenticated if said check token is the same as said authentication token of said second unit***,"

referring to elements 515-517 of Figure 5 and stating that "after receiving W from Alice 509, Bob verifies that W proves that she knows both K1 and K2 515." As should be noted from the prior paragraph, the Examiner's assertion that Jablon teaches the second claim element relies on equating K1 (the "Key shared with Bob" 531) to the claimed "authentication token of the first unit." K1, however, is also the "Key shared with Alice" 532, which is described at column 19, line 54, et seq., as "a shared authenticated value." But, as described supra, the authentication tokens utilized in Applicant's invention are "individualized" (i.e., unique) to each unit and, therefore, are not shared. Therefore, Jablon also fails to teach "**comparing**, at the second unit, **the check token** [**created by the first unit]** ***with the authentication token of the second unit*** for authentication of the first unit towards the second unit, ***wherein said user of said first unit is authenticated if said check token is the same as said authentication token of said second unit***."

In response, the examiner respectfully disagrees. In response to Appellant's argument that the references fail to show certain features of Appellant's invention, it is noted that the features upon which Appellant relies (i.e., the authentication tokens utilized in Applicant's invention are "individualized" (i.e., unique) to each unit and, therefore, are not shared) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Furthermore, Jablon discloses that after receiving W from Alice 509, Bob verifies that W proves that she knows both K_1 and K_2 515. If the verification succeeds, Bob has

proven that Alice knows C and the protocol succeeds 517 (Fig. 5, 515-517). Thus, Bob verifies that W received from Alice includes at least one element that is identical to Bob's one way hidden password S.

On page 8 of the brief, Appellant argues that [f]or the foregoing reasons, claim 1 is not anticipated by Jablon. Whereas independent claims 25 and 41 recite limitations analogous to those of claim 1, they are also not anticipated by Jablon. Furthermore, whereas claims 10, 11, 13, 15-21 and 23 are dependent from claim 1; claims 32 and 34-40 are dependent from claim 25; and claim 45 is dependent from claim 41, and each include the limitations of their respective base claim, they are also not anticipated by Jablon.

In response, the examiner respectfully disagrees. Based on the reasons above, claim 1 is anticipated by Jablon. Since independent claims 25 and 41 recite limitations analogous to those of claim 1, they are also anticipated by Jablon. Claims 10, 11, 13, 15-21 and 23 depend from claim 1, claims 32 and 34-40 depend from claim 25, and claim 45 depends from claim 41 and thus are also anticipated by Jablon.

3) CLAIMS 2, 26 AND 42 ARE PATENTABLE OVER JABLON IN VIEW OF U.S. PATENT NO. 6,721,886 ("USKELA")

On page 8 of the brief, Appellant argues that [a]s established supra, Jablon fails to anticipate independent claims 1, 25 and 41, from which claims 2, 26 and 42 are dependent, respectively. The Examiner has not pointed to any teaching in Uskela to

overcome the deficiency in the teachings of Jablon and, therefore, claims 2, 26 and 42 are not obvious in view of that combination of references.

In response, the examiner respectfully disagrees. Based on the reasons above, independent claims 1, 25 and 41, from which claims 2, 26 and 42 depend respectively are anticipated by Jablon. Thus, claims 2, 26 and 42 are obvious in view of Jablon-Uskela combination.

4) CLAIMS 3, 5, 27, 29 AND 43 ARE PATENTABLE OVER JABLON IN VIEW OF U.S. PATENT NO. 5,778,066 ("HAUSER")

On page 9 of the brief, Appellant argues that [a]s established supra, Jablon fails to anticipate independent claims 1, 25 and 41, from which claims 3, 5, 27, 29 and 43 are dependent. The Examiner has not pointed to any teaching in Hauser to overcome the deficiency in the teachings of Jablon and, therefore, claims 3, 5, 27, 29 and 43 are not obvious in view of that combination of references.

In response, the examiner respectfully disagrees. Based on the reasons above, independent claims 1, 25 and 41, from which claims 3, 5, 27, 29 and 43 depend are anticipated by Jablon. Therefore, claims 3, 5, 27, 29 and 43 are obvious in view of Jablon-Hauser combination.

5) CLAIMS 4 AND 28 ARE PATENTABLE OVER JABLON IN VIEW OF HAUSER AND U.S. PATENT NO. 6,397,329 ("AIELIO")

On page 9 of the brief, Appellant argues that [a]s established supra, Jablon fails to anticipate independent claims 1 and 25, from which claims 4 and 28 are dependent, respectively. The Examiner has not pointed to any teaching in Aielio to overcome the deficiency in the teachings of Jablon and, therefore, claims 4 and 28 are not obvious in view of that combination of references.

In response, the examiner respectfully disagrees. Based on the reasons above, independent claims 1 and 25, from which claims 4 and 28 depend respectively are anticipated by Jablon. Hence, 4 and 28 are obvious in view of Jablon-Hauser-Aiello combination.

6) CLAIMS 7, 8, 31 AND 44 ARE PATENTABLE OVER JABLON IN VIEW OF HAUSER AND U.S. PATENT NO. 6,215,877 ("MATSUMOTO")

On page 9 of the brief, Appellant argues that [a]s established supra, Jablon fails to anticipate independent claims 1, 25 and 41, from which claims 7, 8, 31 and 44 are dependent. The Examiner has not pointed to any teaching in Matsumoto to overcome the deficiency in the teachings of Jablon and, therefore, claims 7, 8, 31 and 44 are not obvious in view of that combination of references.

In response, the examiner respectfully disagrees. Based on the reasons above, independent claims 1, 25 and 41, from which claims 7, 8, 31 and 44 depend are anticipated by Jablon. As a result, claims 7, 8, 31 and 44 are obvious in view of Jablon-Hauser-Matsumoto combination.

7) CLAIM 9 IS PATENTABLE OVER JABLON IN VIEW HAUSER, MATSUMOTO AND U.S. PATENT NO. 6,885,388 ("GUNTER")

On page 10 of the brief, Appellant argues that [a]s established supra, Jablon fails to anticipate independent claim 1, from which claim 9 is dependent. The Examiner has not pointed to any teaching in Gunter to overcome the deficiency in the teachings of Jablon and, therefore, claim 9 is not obvious in view of that combination of references.

In response, the examiner respectfully disagrees. Based on the reasons above, independent claim 1 from which claim 9 depends is anticipated by Jablon. Thus, claim 9 is obvious in view of Jablon-Hauser-Matsumoto-Gunter combination.

8) CLAIM 14 IS UNPATENTABLE OVER JABLON IN VIEW OF U.S. PATENT NO. 7,363,494 ("BRAINARD")

On page 10 of the brief, Appellant argues that [a]s established supra, Jablon fails to anticipate independent claim 1, from which claim 14 is dependent. The Examiner has not pointed to any teaching in Brainard to overcome the deficiency in the teachings of Jablon and, therefore, claim 14 is not obvious in view of that combination of references.

In response, the examiner respectfully disagrees. Based on the reasons above, independent claim 1 from which claim 14 depends is anticipated by Jablon. Therefore, claim 14 is obvious in view of Jablon-Brainard combination.

9) CLAIM 22 IS PATENTABLE OVER JABLON IN VIEW OF HAUSER AND U.S. PATENT NO. 6,668,167 ("MCDOWELL")

On page 10 of the brief, Appellant argues that [a]s established supra, Jablon fails to anticipate independent claim 1, from which claim 22 is dependent. The Examiner has not pointed to any teaching in McDowell to overcome the deficiency in the teachings of Jablon and, therefore, claim 22 is not obvious in view of that combination of references.

In response, the examiner respectfully disagrees. Based on the reasons above, independent claim 1 from which claim 22 depends is anticipated by Jablon. Thus, claim 22 is obvious in view of Jablon-Hauser-McDowell combination.

10) CLAIM 24 IS PATENTABLE OVER JABLON IN VIEW OF U.S. PATENT NO. 7,076,656 ("MACKENZIE")

On pages 10-11 of the brief, Appellant argues that [a]s established supra, Jablon fails to anticipate independent claim 1, from which claim 24 is dependent. The Examiner has not pointed to any teaching in MacKenzie to overcome the deficiency in the teachings of Jablon and, therefore, claim 24 is not obvious in view of that combination of references.

In response, the examiner respectfully disagrees. Based on the reasons above, independent claim 1 from which claim 24 depends is anticipated by Jablon. Therefore, claim 24 is obvious in view of Jablon-McKenzie combination.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Trong Nguyen/

Examiner, Art Unit 2436

Conferees:

/Eleni A Shiferaw/

Primary Examiner, Art Unit 2436

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436